

# **SCRAMDISK v2.02C USER MANUAL**

**FREE HARD DRIVE ENCRYPTION  
FOR WINDOWS 95 & 98**

**[http://www.hertreg.ac.uk/ss/  
scramdisk@hotmail.com](http://www.hertreg.ac.uk/ss/scramdisk@hotmail.com)**

# Contents

<b>CONTENTS</b> .....	<b>2</b>
<b>DISCLAIMER:</b> .....	<b>3</b>
<b>INTRODUCTION</b> .....	<b>4</b>
SYSTEM REQUIREMENTS .....	4
INSTALLING SCRAMDISK .....	5
REMOVING SCRAMDISK .....	5
<b>USING SCRAMDISK</b> .....	<b>6</b>
CREATING AN ENCRYPTED VOLUME .....	7
CREATING AN ENCRYPTED PARTITION .....	10
MOUNTING AN ENCRYPTED VOLUME .....	13
MOUNTING AN ENCRYPTED PARTITION .....	15
ACCESSING AN ENCRYPTED VOLUME .....	16
DISMOUNTING ENCRYPTED VOLUMES .....	17
SETTING PREFERENCES FOR AN ENCRYPTED VOLUME .....	18
USING THE TIMEOUT FEATURE .....	20
VERIFYING THE ALGORITHMS USED .....	22
2ND USER ACCESS - SAVING A KEYFILE .....	23
2ND USER ACCESS - MOUNTING ENCRYPTED VOLUMES .....	24
ASSOCIATE CONTAINER AND KEYFILES WITH SCRAMDISK .....	25
MOUNTING ENCRYPTED VOLUME(S) OR PARTITION(S) AT START-UP .....	26
COMMAND LINE ACCESS .....	27
<b>SCREEN AND MENU DESCRIPTIONS</b> .....	<b>28</b>
THE MAIN SCREEN .....	29
PASSWORD AND CONFIRM PASSWORD SCREENS .....	30
THE RED LOW LEVEL MESSAGE SCREEN .....	31
DESCRIPTION OF MENU OPTIONS .....	32
<b>TECHNICAL OVERVIEW</b> .....	<b>41</b>
THE ENCRYPTION PROCESS .....	41
SUPPORTED ENCRYPTION ALGORITHMS .....	42
ALGORITHM SUMMARY .....	43
<b>FREQUENTLY ASKED QUESTIONS (FAQ)</b> .....	<b>44</b>
<b>PROGRAM RATIONALE</b> .....	<b>50</b>
<b>FUTURE DEVELOPMENTS</b> .....	<b>51</b>
<b>PROGRAM REVISIONS</b> .....	<b>52</b>
PROGRAM VERSIONS .....	52
BUGS .....	53
<b>LICENSE DETAILS</b> .....	<b>54</b>
IDEA CONDITIONS OF USE AND REQUIRED NOTICE: .....	54
<b>RESOURCES</b> .....	<b>56</b>
CRYPTOGRAPHY AND INFORMATION SECURITY .....	56
WIDER ISSUES .....	56
<b>GREAT CRYPTO &amp; INFO SECURITY QUOTES</b> .....	<b>58</b>
<b>CONTACTING THE AUTHOR</b> .....	<b>63</b>
<b>ACKNOWLEDGEMENTS</b> .....	<b>63</b>
<b>APPENDIX A ALGORITHM TEST VECTORS</b> .....	<b>64</b>

## Disclaimer:

This program employs disk volume scrambling methods to prevent unauthorised access of stored data, which may be interpreted by some as being 'encryption', and therefore the use of this program may be restricted or forbidden in some countries.

It is not intended for use of storage of data illegal in your country, and such use is not the purpose of the program writers, in providing this utility software.

The program writers (who wish to remain anonymous) cannot be responsible for loss of data, due to any incompatibility of the program, running on any particular hardware, and/or software configuration.

By using the program, the person installing it, acknowledges their **own** responsibility to back up their important data, and is here advised to do so, before the installation of this software.

It is a condition of use, that data loss owing to any bug, error or failure of this program is not the responsibility of the program writers. If in doubt, backup your data before installation of this software, and if possible satisfy yourself of its current operation on a system which doesn't contain irreplaceable data.

The program writers cannot be responsible, or render any assistance, in the event of loss of passphrase needed to access scrambled data.

## Introduction

ScramDisk is a program that provides a virtual encrypted disk on Windows 95 & 98 machines. Basically, a container is created on the hard disk that is then mounted by the ScramDisk software. This software creates a new logical drive letter through which the disk is accessed. The important thing is that any data written to the new logical drive is encrypted with the algorithm of your choice.

This document doesn't include an introduction into the way encryption works.

There are existing programs that already provide this functionality under Windows 95 & NT, but ScramDisk is currently unique for a number of reasons:

1. It is a fully functional virtual disk based encryption system that runs under both Windows 95 and Windows 98.
2. It is free to use with absolutely no restrictions.
3. The source code is available for peer-review and further program development with very few conditions (See the section License Details).
4. It has been developed in the UK and, for the time being at least, can be exported electronically from the UK. Even if the law changes in the future, it is hoped that ScramDisk will by then be widely disseminated.
5. It is impossible to prove that a large file held on a drive is a ScramDisk virtual disk container without knowing the pass-phrase. The ScramDisk container files do not have to have a standard file extension and contain no file headers that indicate the file is anything but random data. Use the program DieHard to test the 'randomness' of a ScramDisk virtual disk.
6. It can be seen as a work in progress. It is hoped that people with the correct skills will take the software and enhance the functionality by adding both new features and new encryption algorithms. The program includes an extensible architecture, which enables new algorithms to be added with minimal fuss.
7. The program executables are very small and can be carried on a 3 1/2" floppy disk.
8. The program allows you to hide a file-system in a WAV file. This is known as steganography.

## System Requirements

ScramDisk has very meagre system requirements in order to run:

- A PC capable of running Windows 95 or 98
- At least 1Mb of free disk space for the ScramDisk installation.
- Space to create the ScramDisk volume files. This could be either space on a FAT16 or FAT32 drive, a blank partition, or a large WAV file in the case of steganography.

That's it!

## ***Installing ScramDisk***

ScramDisk is distributed as a ZIP file named SDisk.zip, which is downloadable from the ScramDisk homepage (<http://www.hertreg.ac.uk/ss/>). Once the zip file has been downloaded you need to extract the file to a suitable directory (for example 'c:\scramdisk\').

**Known Problem:** Do not try to install ScramDisk into the same directory that it was extracted.

Now run the file 'installdir\sdinstal.exe' and follow the instructions. Once the installation is complete the system will restart. Once the system has restarted you will then be able use the ScramDisk program to create and access encrypted volumes.

In the very unlikely event of complete system failure immediately after installation do the following:

1. Boot to DOS using the appropriate function keys
2. Delete the file "C:\Windows\SYSTEM\IOSUBSYS\SD.VXD"
3. Restart windows. The scramdisk won't work however as the driver will have been removed.

The path above assumes your windows directory to be "C:\Windows\", if it isn't then use the correct windows directory.

## ***Removing ScramDisk***

Load the ScramDisk application and choose the menu option 'File | Uninstall ScramDisk...'. You will be asked if you really wish to remove the ScramDisk program and the program will then restart the computer.

## Using ScramDisk

This part of the documentation provides step-by-step guides to using the major features of ScramDisk.

Where there is more than one way to do something, the guide will give you each of the possible courses and the appropriate actions for each.

To get the most from this guide, it is worth spending a moment familiarising yourself with the conventions employed, as explained in the next paragraph.

### Conventions

Items in **bold** refer to screen items; they may be a menu title, a menu entry or just an option in a dialogue box. When you encounter a **bold** entry, look at the ScramDisk screen and you should see the item there.

Items in [brackets] are usually the titles of sections within dialogue boxes, they will also be in **bold** because they are items that are present on the screen.

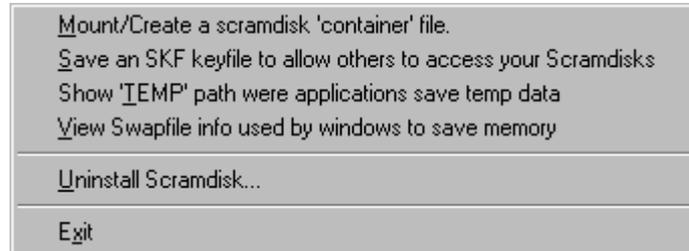
Items in `monospaced font` are command line entries, they are text that is typed directly at a DOS-box prompt.

Alternative courses of action are nested within the description of the parent process. Thus a course of action which can be performed in several ways will have –OR– as a separator between the different possibilities. This carries down so that further options are nested within the main possibilities. Look for different levels of indentation as a guide to this.

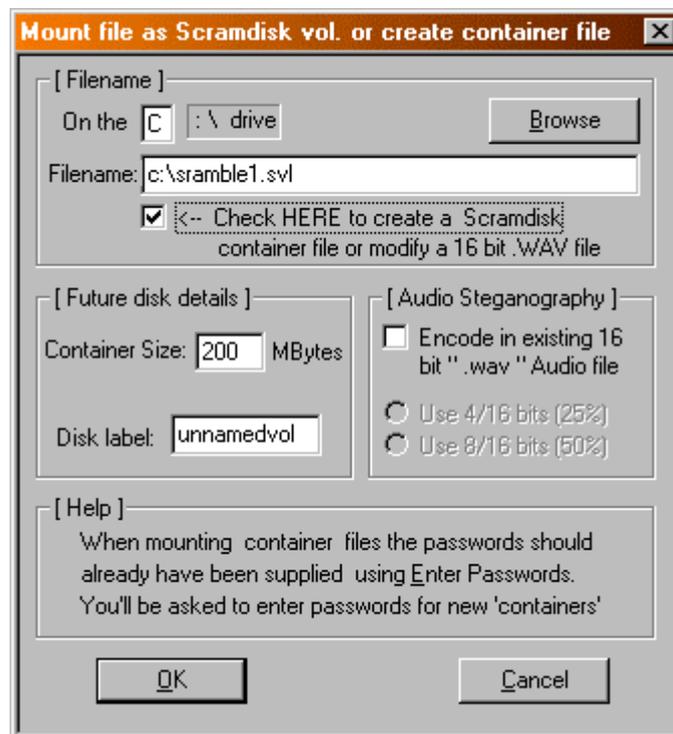
## Creating an Encrypted Volume

At the main screen:

From the **File** menu, choose **Mount/Create a ScramDisk 'container' file**.



Fill in the resulting dialogue box according to the following instructions:



In the **[Filename]** section:

Tick the "**Click HERE to create a ScramDisk container file or modify a 16bit .WAV file**" checkbox.

Enter the path for the encrypted volume as a combination of Drive and Filename (Filename may include directory path as well).

-OR-

If you wish to use Audio Steganography, enter the path to a suitable wave file or click the **Browse** button to locate it.

In the **[Future disk details]** section:

Enter the size for the new volume (in Megabytes).

Give the volume a label, exactly as you would an ordinary logical drive.

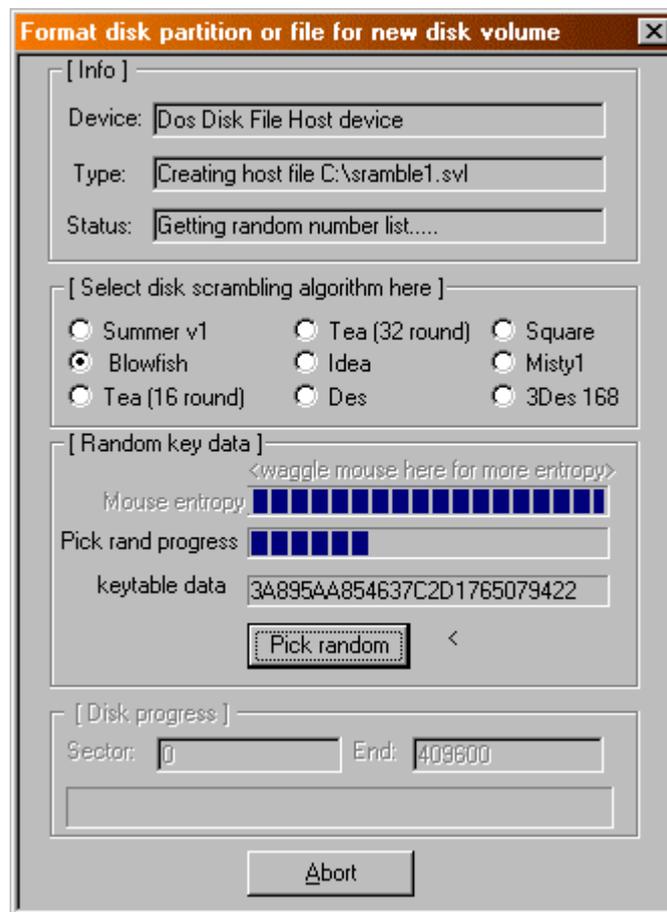
-OR-

In the **[Audio Steganography]** section:

Check the **Encode in existing 16bit** box.

Choose either to use either the least 4 or 8 bits of the file for the encrypted volume. This will give you an Encrypted Volume with a size equal to 25% or 50% of that of the Wave file, respectively.

Click the **"OK"** button to move to the Format screen.



In the section **[Select disk scrambling algorithm here]:**

Choose the algorithm you wish to be used in the encryption of the volume.

In the section **[Random Key data]:**

Move the mouse until a good portion, or preferable all, of the **Mouse entropy** gauge is filled.

Click the **Pick random** button until the **Pick rand progress** gauge is full.

-OR-

Click the **Pick random** button once, to pass the focus to it, then press the space bar until the **Pick rand progress** gauge is full.

In the Password screen:

Enter the passphrase be used by the algorithm.

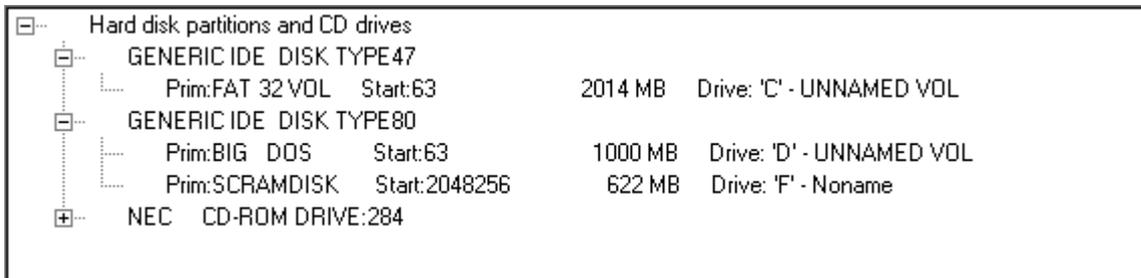
You will then be required to re-enter the passphrase to confirm it.

N.B. This phrase will be required to access the encrypted volume in future, so make sure you remember it and the positions in which you entered it!

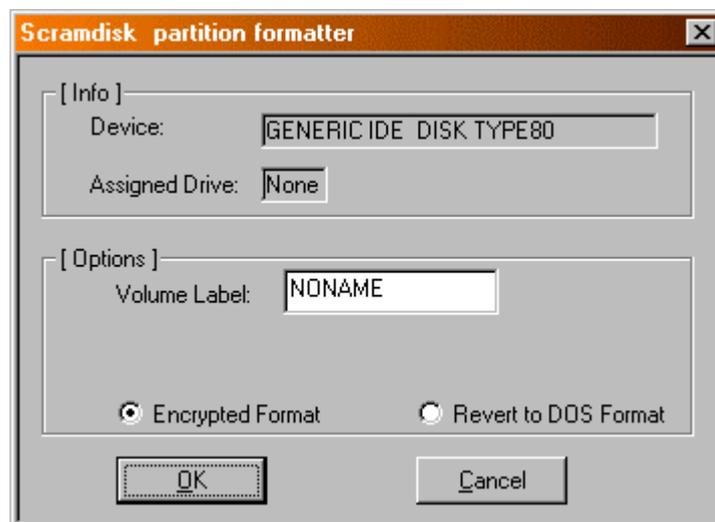
The volume will now be created by ScramDisk. This may take some time, depending upon the size of the volume.

## Creating an Encrypted Partition

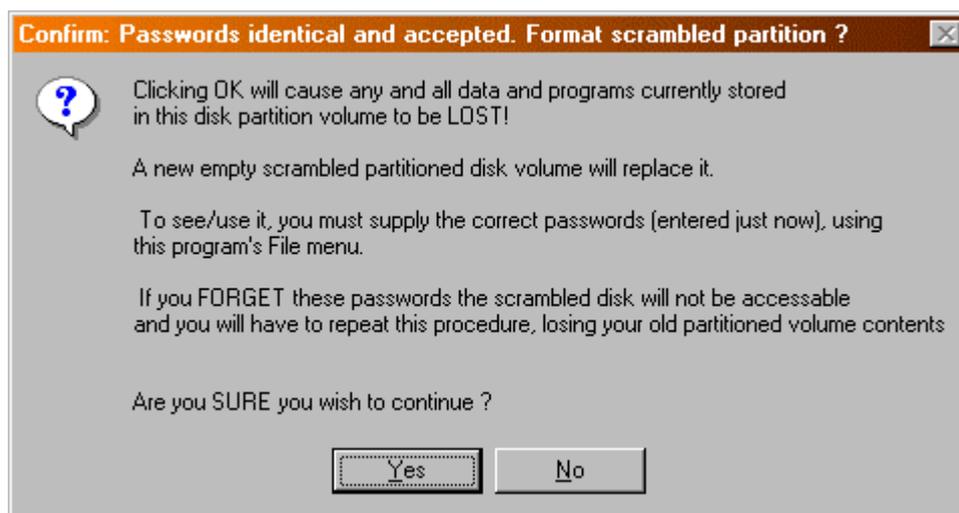
In the centre portion of the main screen (see Screen descriptions further on in this guide) there is displayed a list of the devices attached to the system.



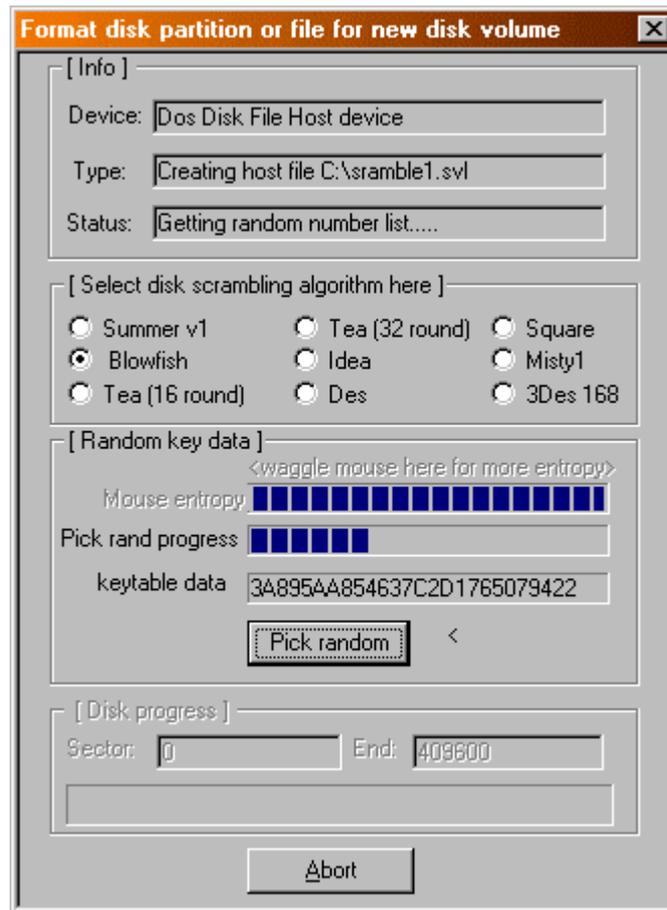
Double-click on the partition you wish to format with ScramDisk and a dialogue box will appear.



Choosing **Encrypted Format** and clicking OK will bring up a confirmation box.



Clicking **Yes** in this box will take you to a Dialogue box which is common to all the methods of creating encrypted volumes.



In the section **[Select disk scrambling algorithm here]:**

Choose the algorithm you wish to be used in the encryption of the partition.

In the section **[Random Key data]:**

Move the mouse until a good portion, or preferable all, of the **Mouse entropy** gauge is filled.

Click the **Pick random** button until the **Pick rand progress** gauge is full.

-OR-

Click the **Pick random** button once, to pass the focus to it, then press the space bar until the **Pick rand progress** gauge is full.

In the **Password** screen:

Enter the passphrase be used by the algorithm.

You will then be required to re-enter the passphrase to confirm it.

N.B. This phrase will be required to access the encrypted partition in future, so make sure you remember it and the positions in which you entered it!

The partition will now be formatted by ScramDisk. This may take some time, depending upon the size of the partition and the algorithm chosen.

## Mounting an Encrypted Volume

At the main screen:

From the **P**asswords menu, choose **E**nter ciphered disk volume passwords



Enter the passphrase that you chose when you created the encrypted volume, in the same lines that you first entered it.

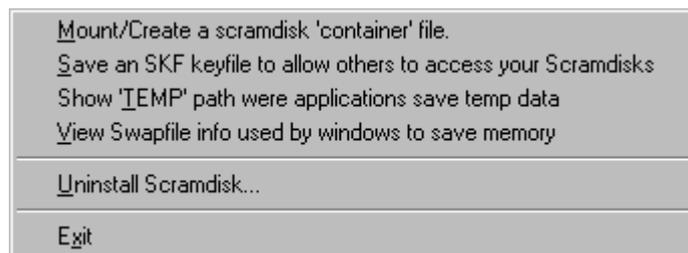
If you have associated the .SVL extension with ScramDisk (see How To... Associate extensions), double-click the filename in an Explorer / Open window.

-OR-

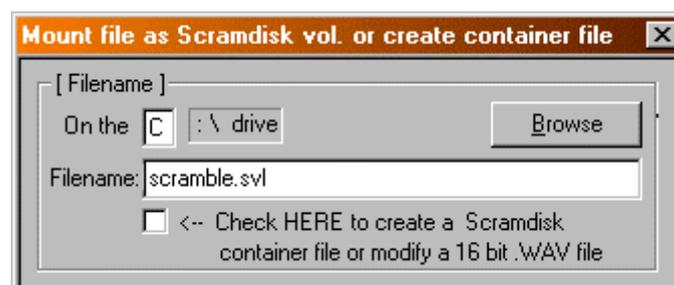
Drag the Encrypted Volume file from an Explorer / Open window and drop it on an empty slot.

-OR-

From the **F**ile menu, choose **M**ount/Create a ScramDisk 'container' file



Fill in the resulting dialogue box according to the following instructions:



In the **[Filename]** section:

Enter the path for the encrypted volume as a combination of Drive and Filename (Filename may include directory path as well, but not drive letter).

-OR-

Click the **B**rowse button to locate it.

Make sure that the "**Click [HERE](#) to create a ScramDisk container file or modify a 16bit .WAV file**" checkbox is not ticked, then click the **OK** button to finish mounting the volume.

The mounted volume will now appear in the first free slot in the Main Screen.

N.B. See the instructions for setting volume preferences to alter the way the volume is presented.

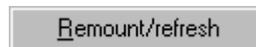
## Mounting an Encrypted Partition

Enter the passphrase for the partition by choosing “**Enter ciphered disk volume passwords**” from the **P**asswords menu.



If you have left the “**Don t scan HD partitions after entering passwords**” option un-checked in the **T**imeout and **O**ther **S**ettings dialogue box, then ScramDisk will mount any partition that the passwords have been entered for automatically.

If not, you must choose **R**emount/**R**efresh from the **P**artitions menu to make ScramDisk mount the partition.



## ***Accessing an Encrypted Volume***

Run ScramDisk and follow the instructions for mounting a volume.

The volume can now be accessed in a number of ways:

From the Main Screen click on the mounted volume icon (see Main Screen description for further details).

-OR-

From Explorer / File Manager in the same way that any drive is accessed.

-OR-

From any file dialogue box, e.g. The **Start** menu **Run** command, the **File Open** dialogue box in any Microsoft Office application etc.

-OR-

From an MS-DOS box use the drive letter of the volume exactly as you would a local hard drive.

Operation of the encrypted volume is transparent to the user and application, save for a small performance drop, the magnitude of which is dependant upon the algorithm used and computational power of the PC.

Encrypted Volumes remain accessible until Windows is next shutdown. Since the VxD component is always loaded, you do not need to keep the ScramDisk utility running once the Encrypted Volumes have been mounted.

## ***Dismounting Encrypted Volumes***

At the main screen:

From the **Dismount** menu,



Choose **Dismount All**, to dismount all the currently Mounted Volumes.

-OR-

Choose **Dismount Brutal**, to brutally dismount all the mounted volumes. This will cause all volumes to be dismounted regardless of any open files or windows. ScramDisk will wait until 2 seconds have elapsed since the last I/O operation on the Volume, to allow for pending writes etc.

-OR-

If you wish to dismount a particular volume but leave the others mounted, right-click the Volume's icon in the main screen and click the **Dismount** button in the **Volume info** dialogue box.

## Setting Preferences for an Encrypted Volume

At the main screen:

Right-Click on the slot with the mounted volume you wish to set preferences for to bring up the "**Scrambled Volume info**" dialogue box.



In the [**Editable Info Text**] section:

Add comments to describe the volume (optional).

Enter a drive letter that you would prefer the volume to be mounted as. If none is entered then the volume is assigned the first available letter at the time it is mounted.

Click the **New Password** button to change the passphrase for the Volume.

Click the **Revoke SKF** button to revoke the rights any previously created SKF files have to access the Volume.

Click the **Update** button to save your preferences for the volume.

N.B. If you are going to run an application from within the volume, that has registry entries associated with it, then you should make sure the same letter is always assigned and available. A good way to do this is to choose a drive letter well into the alphabet (E.G. X:) to prevent a clash with your CD-ROM or other volumes.

This section also gives information on when the volume was last successfully mounted and how many times it has been successfully mounted so far.

The [**Data information**] section summarises the Encryption Algorithm, Encrypted Volume Storage name and the Steganography used (if any).

You can also explore or dismount the volume from this screen by clicking the **Explore** or **Dismount** buttons.

N.B. If you have changed the preferred drive letter for the volume, you must dismount and remount it for the change to be effected.

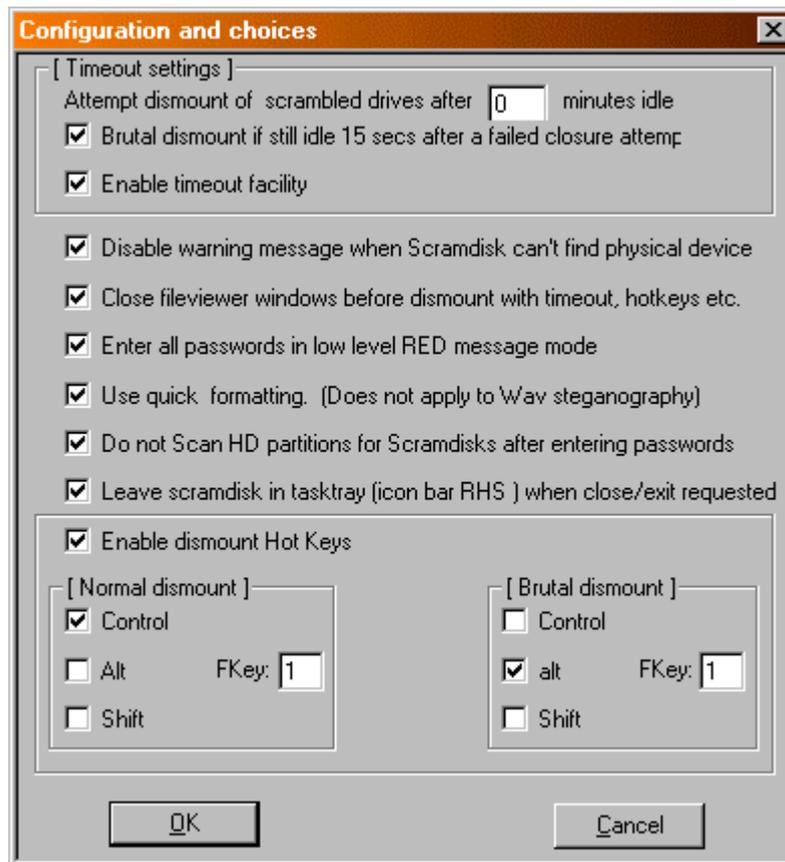
## Using the Timeout Feature

At the main screen:

From the **Timeout/Configure** menu, choose **Timeout and other Setups...**



In the resulting dialogue box,



Check the **"Enable timeout facility"** box to activate this feature.

In the **[Timeout settings]** section:

Enter the period of idle time (in minutes) that you want ScramDisk to wait before it attempts to dismount all mounted volumes. This may fail if there are open files from or windows on the Encrypted volume(s).

Check the **"Brutal dismount if still idle 15 secs after a failed closure attempt"** checkbox if you want ScramDisk to forcibly dismount the volumes. This will happen 15 seconds after the first attempt if ScramDisk failed on that occasion.

Other settings that affect the Timeout Feature are:

**"Close fileviewer windows before dismount with timeout, hotkeys etc."**.

Check this if you want ScramDisk to close any Explorer type windows that are open on encrypted volumes when it attempts to dismount them.

Choosing this option makes it more likely that ScramDisk will dismount Volumes gently and hence successfully.

### **"Enable dismount Hot Keys"**

Check this box if you want to be able to cause ScramDisk to dismount all Encrypted Volumes at the press of a key.

For this to work you must check the "**Leave ScramDisk in tasktray...**" box which is also in this dialogue box.

Once "**Enable dismount Hot keys**" has been selected you may use the options in the "**Normal dismount**" and "**Brutal dismount**" sections to choose key combinations for the Hot Keys.

Other Settings in this dialogue box are explained elsewhere in this guide.

## Verifying the Algorithms Used

Obtain a reliable set of plaintext, key and ciphertext for the algorithm you wish to verify.

At the main screen:

From the **About** menu, choose **Cipher verifier**. This will bring up the verifier utility.

**Cipher algorithm verification**

[ Hexadecimal key ]

00000000 00000000 00000000 00000000  
Long 0 Long 1 Long 2 Long 3

[ Hexadecimal plaintext ]

00000000 00000000 [ ] [ ]  
Long 0 Long 1 Long 2 Long 3

[ Hexadecimal ciphertext ]

00000000 00000000 [ ] [ ]  
Long 0 Long 1 Long 2 Long 3

[ Cipher Algorithm to verify ]

Blowfish \*  Tea 16r  Tea 32r  Idea  
 Des 56bit  Square  Misty1

\*Test blowfish key len. is 128 bits. The program uses 256 bits

Read byte values from left to right in memory order

Exit Clear **Encrypt** Decrypt

In the **[Hexadecimal key]** section:

Enter your 'known good' key.

In the **[Hexadecimal plaintext]** section:

Enter your 'known good' plaintext.

In the **[Cipher Algorithm to verify]** section:

Choose the algorithm to be tested by clicking the radio button beside it.

Press the **Encrypt** button.

Check the values in the **[Hexadecimal ciphertext]** section against your 'known good' ciphertext.

N.B. The reverse may also be tested by entering "known good" ciphertext and using the **Decrypt** button to produce the plaintext for comparison

See the section "Appendix A – Algorithm Test Vectors" on page 64 for details of published test vectors.

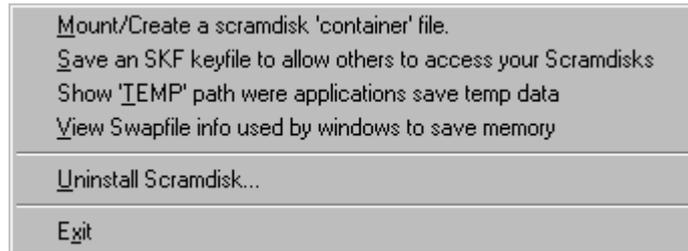
## 2nd User Access - Saving a Keyfile

Mount all the Encrypted Volumes that you wish the second user to be able to access. Instructions for doing this are under "**How To Mounting an Encrypted Volume**".

Enter the passphrase for the keyfile. This is the only passphrase the 2nd user will need or see.

At the main screen:

From the **File** menu, choose **Save an SKF keyfile to allow others to access your Scramdisks**.



Give the Keyfile a name and save it to any location you wish.

The Keyfile is portable, but applies only to the system it was saved from and then only to the volumes that were mounted when it was saved.

A Keyfile's purpose is to allow others access to an Encrypted Volume without needing to let them know the passphrase for the volume itself.

N.B. Keyfile access to a volume can be revoked at a later date from the Volume information dialogue box.

Access via a Keyfile does not allow the user to access to the volume properties dialogue box, the volumes must be mounted with their own passphrase(s) for this to be accessible. Exceptions to this are Summer encrypted volumes whose Keyfiles still allow access to the Properties Dialogue box.

## 2nd User Access - Mounting Encrypted Volumes

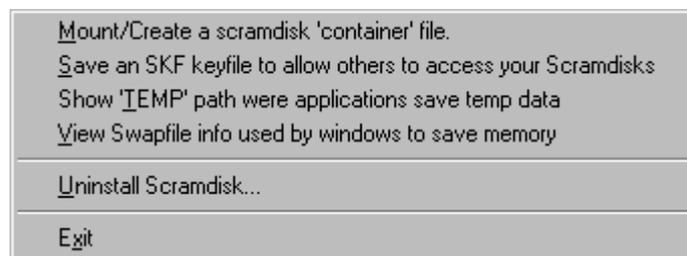
At the main screen:

From the **Passwords** menu, choose **Enter Keyfile password [SKF access files]**, this will bring up the password entry screen.

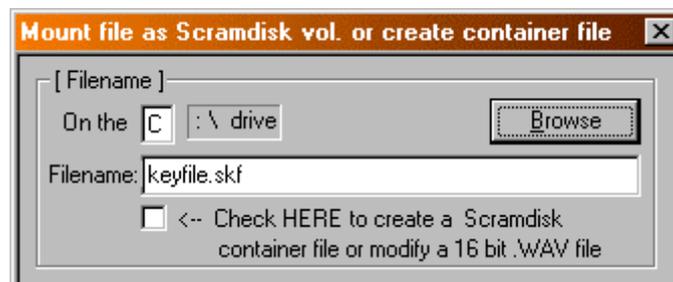


Enter the passphrase that you chose when you created the Keyfile volume, on the same lines that you originally entered it.

From the **File** menu, choose **Mount/Create a ScramDisk 'container' file.**



Fill in the resulting dialogue box according to the following instructions:



In the **[Filename]** section:

Enter the path for the Keyfile as a combination of Drive and Filename (Filename may include directory path as well, but not drive letter).

-OR-

Click the **Browse** button to locate it.

Make sure that the "**Click HERE to create a ScramDisk container file or modify a 16bit .WAV file**" checkbox is not ticked, then click the **OK** button.

The mounted volume(s) will now appear in the slot(s) in the Main Screen.

N.B. Keyfiles created with an earlier version of Scramdisk cannot be opened by V2.02. You should first revoke them (See How To... Setting preferences for an encrypted volume) and then recreate them using V2.02.

## **Associate Container and Keyfiles with ScramDisk**

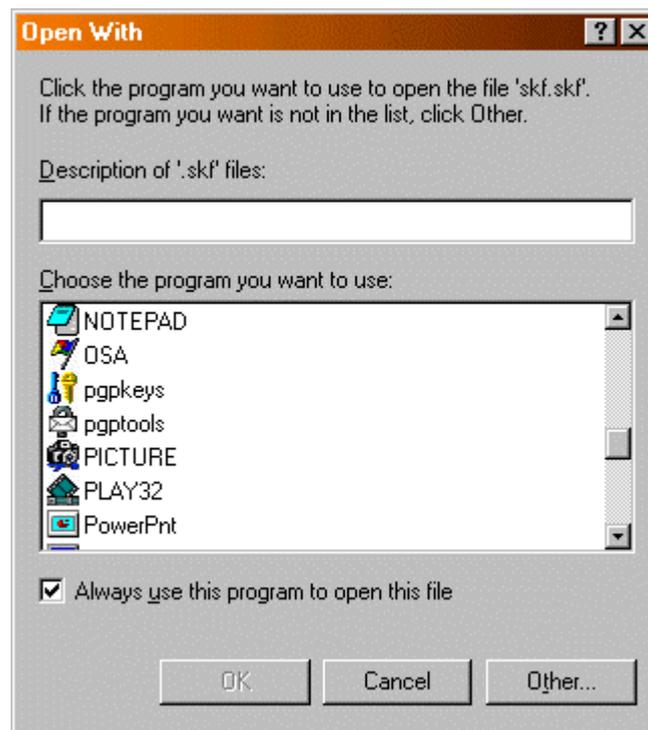
Open **Explorer** or **My Computer** and browse to an Keyfile (.skf) or a container file (.svl) file.

Left-click the file to select it (the name will then be in inverse text).

Hold down Shift and right-click the file icon.

Choose **Open With** from the menu that pops up.

A dialogue box will open:



Click the **Other** button and browse to the location of the ScramDisk.exe file (If you don't know where it is then use **Find** on the **Start** menu to locate it).

Select the ScramDisk.exe file and **OK** it.

Make sure that **Always use this program to open this file** is checked and ScramDisk is selected in the **Choose the program you want to use section**.

**OK** the choices.

When you next click on a Keyfile or container file, ScramDisk will open and request a passphrase (if it is not already cached).

## Mounting Encrypted volume(s) or partition(s) at start-up

There are two different mechanisms for mounting volumes at start-up, which one you use will depend on the number and type of volumes you wish to mount.

For either method to work you must have first associated the file type with the ScramDisk executable. To find out how to do this read the section entitled "How To... Associate Container and Keyfiles with ScramDisk"

Use the table below to decide method is appropriate to you.

Encrypted Volume(s)	Method
Single, file container (.svl) type Volume	1 - Shortcut to file name
Multiple file container (.svl) volumes	2 - Shortcut to SKF file
Steganographic (.wav) volume(s)	2 - Shortcut to SKF file
Encrypted partition(s)	2 - Shortcut to SKF file

### METHOD 1 SHORTCUT TO FILE NAME:

Open the **Start Menu** by right-clicking the **Start** button.

Browse to the **StartUp** folder (it's inside **Programs**).

Right-click on a blank space in the folder.

Choose **N**ew and then choose **S**hortcut from the menu that pops up.

Enter the path to your container (.svl) file in the **Command Line** box and **OK** it.

Give the shortcut a name and **OK** it.

Next time you start Windows, ScramDisk will open and request the passphrase for your container file.

Once entered, your Encrypted Volume will be accessible.

### METHOD 2 SHORTCUT TO SKF FILE:

First mount all the container files and partitions that you wish to mount at start-up.

Save an SKF file according to the instructions in the "How To... 2<sup>nd</sup> User Access - Saving a Keyfile" section.

Follow **Method 1** but enter the path to your Keyfile instead of the path to a container file.

When you next start Windows ScramDisk will open and request the Passphrase for the Keyfile.

Once entered, your Encrypted Volume(s) will be accessible.

## Command Line Access

ScramDisk supports the passing of parameters via the command line for the following actions:

Action	Parameter	Example
Mount <sup>1</sup>	Path to volume	SCRAMDISK.EXE C:\myvolume.svl
Mount <sup>1a</sup>	Path to file	SCRAMDISK.EXE C:\mykeyfile.skf
Normal Dismount	/DN	SCRAMDISK.EXE /DN
Brutal Dismount <sup>2</sup>	/DB	SCRAMDISK.EXE /DB

<sup>1</sup> ScramDisk will attempt to mount the specified volume with currently cached passwords. If the password(s) are not valid or none are cached, then the Password Screen will appear.

<sup>1a</sup> ScramDisk will open all volumes that the Keyfile was made for. You only get one chance to enter the password, if you get it wrong you must run the command again.

<sup>2</sup> Brutal Dismount will not dismount the volume(s) until there have been 2 seconds since the last I/O operation.

N.B. The parameters can be used with a shortcut to the ScramDisk executable (ScramDisk.EXE), but you must include the path to a volume in double quotes if it has spaces in it.

## Screen and Menu Descriptions

This part of the documentation provides descriptions of the most frequently used screens and all the Main Screen menus.

The most frequently used screens are represented by a screen shot and accompanying text which explains the elements found in the screen.

All the menus from the Main Screen are represented by a screen shot and a description of the actions of each of its items.

### Conventions (Menu descriptions)

**Bold** items refer to menu options themselves.

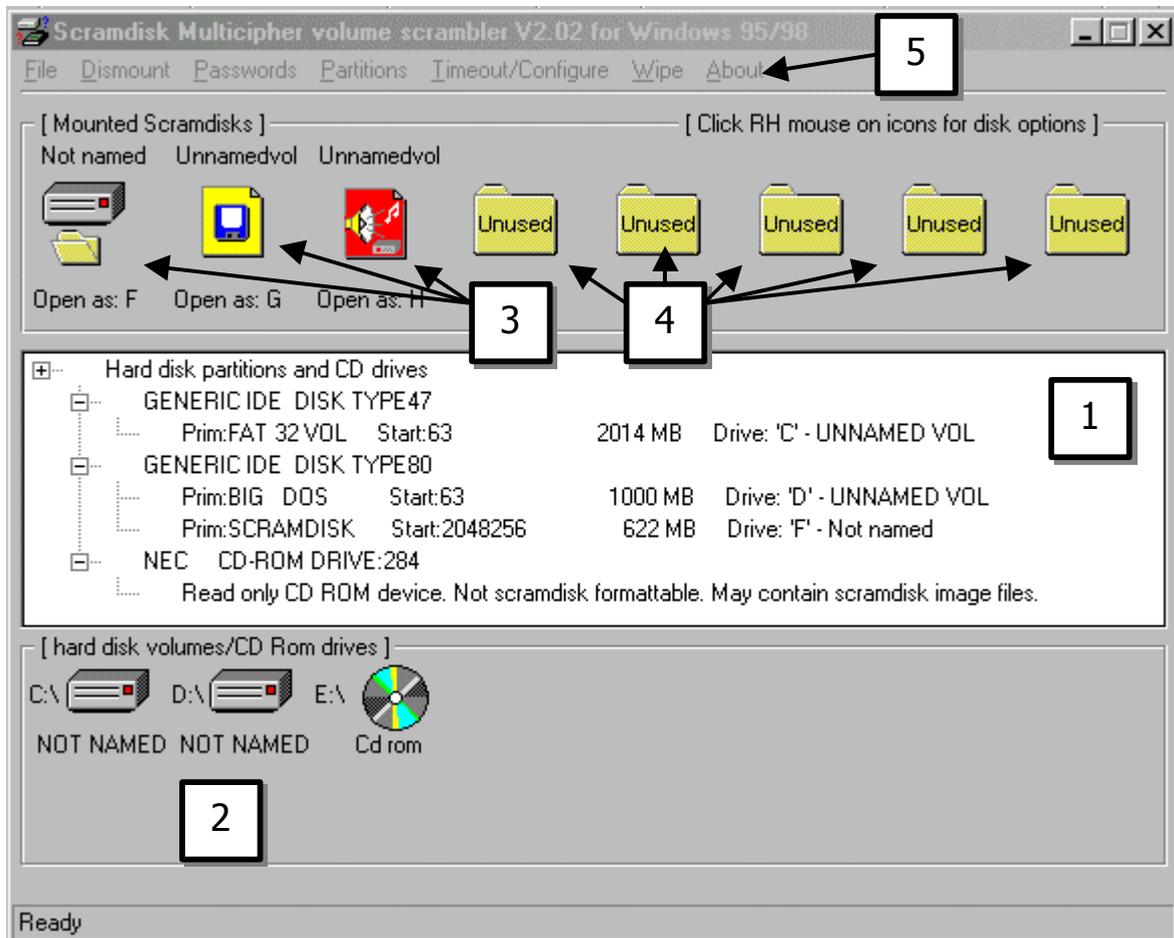
The text for each item is set as an indented paragraph.

Thus the overall style is:

**MENU ITEM** (**bold, SMALL CAPS**)

Description of item. (indented)

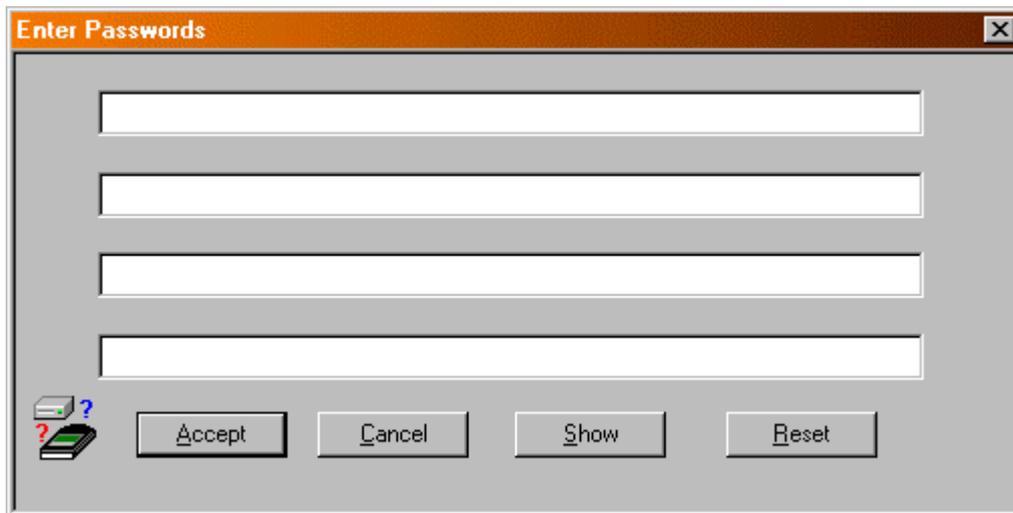
## The Main Screen



Key to Figure:

- 1** This area displays the devices attached to the system
- 2** This area displays the first 16 Hard Disk volumes and CD ROMs attached to the system.  
Left-Clicking an icon opens that volume.  
Right-Clicking an icon opens that volume in an Explorer window.
- 3** This area shows mounted volumes and available slots.  
Example **3** shows 3 mounted volumes (A partition, container file and stegonographic wave container, respectively). Example **4** shows 5 empty slots.
- 4** Left-Clicking on an empty slot brings up the password entry screen, readying the slot for a volume to be mounted.  
Left-Clicking on an occupied slot opens the volume.  
Right-Clicking on an occupied slot displays the volume info dialogue box.
- 5** Menus.  
See following pages for individual descriptions.

## Password and Confirm Password Screens

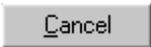
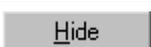


### [Disk volume passwords]:

This section contains 4 text boxes, for entering your passphrase, you may use as many or as few of the 4 lines as you need.

Use the **Tab** and **Shift-Tab** key(s) to move between the 4 text boxes.

### Buttons:

	Saves the passwords entered and closes the dialogue box.
	Closes the dialogue box with no action taken.
	Toggle between displaying passwords as asterisk placeholders or plain-text.
	
	Clears all the text boxes.

N.B. With the exception of the title-bar text, the Confirm Passwords Screen and keyfile Password Screen are identical to the Password Screen.

## **The Red Low Level Message Screen**

This feature is designed to avoid the possibility of keyboard messages, between Windows and the application, being copied by another programme or process.

When enabled in the "**Timeout/Configure**" settings, this feature takes over from the normal windows password entry screens.

Instead you will be presented with a red screen, rather CGA like in appearance.

The screen serves exactly the same function as the windows password screens, with keys taking the place of buttons according to the following rubric:

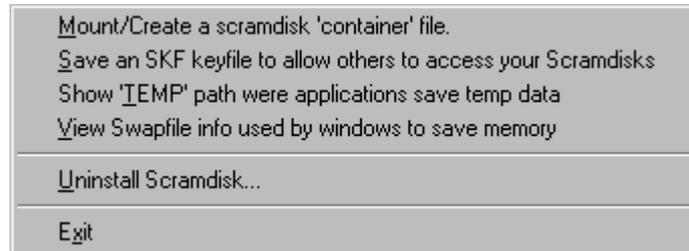
<b>Key</b>	<b>Button</b>
Enter	Accept
PageDown	Show
PageUp	Hide
Escape	Cancel
Home	Reset

In addition to the above keys, F1 enters a | (pipe) symbol and F2 enters a # (hash).

**This feature should not be used when a keyboard other than a standard QWERTY type is used (e.g. a French keyboard).**

## Description of menu options

### File



#### **MOUNT/CREATE A SCRAMDISK 'CONTAINER' FILE:**

Used to create a new encrypted volume or to mount an already present one. See 'How To.. Mount an Encrypted Volume' for full usage.

#### **SAVE AN SKF KEYFILE TO ALLOW OTHERS TO ACCESS YOUR SCRAMDISKS:**

See the "How To.. 2<sup>nd</sup> User Access" sections.

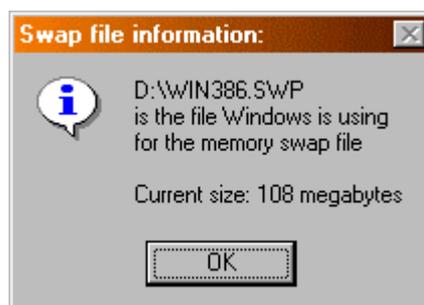
#### **SHOW 'TEMP' PATH WHERE APPPLICATIONS SAVE TEMP DATA:**

Display the path to the directory where temporary data is saved by applications (the value of the TEMP environment variable), and allows you to explore that directory.



Data saved here is not encrypted and therefore represents a possible avenue for data theft.

#### **VIEW SWAPFILE INFO USED BY WINDOWS TO SAVE MEMORY:**



Windows 'pages' out data from memory that is not needed immediately to disk, as means of providing 'Virtual Memory'.

Data saved in this 'virtual memory' swapfile is not encrypted and therefore represents a possible avenue for data theft.

See also the **Wipe Menu** section for help on wiping the swap file slack.

**UNINSTALL SCRAMDISK:**

Completely removes the ScramDisk programme and driver from the system.

**EXIT:**

Exits ScramDisk, offering you the choice of whether to clear the password cache before doing so.

N.B. Your Encrypted volumes will still be accessible until you restart windows or use ScramDisk to dismount them.

## Dismount



### **DISMOUNT ALL:**

Dismounts all mounted volumes.

### **DISMOUNT BRUTAL:**

Brutally dismounts all the mounted volumes.

See “How To... Dismounting Encrypted Volumes” for more information.

## Passwords



### **ENTER CIPHERED DISK VOLUME PASSWORDS:**

Brings up a dialogue box for entering your passphrase in preparation for mounting or creating an Encrypted Volume.

### **ENTER KEYFILE PASSWORD (SKF ACCESS FILES):**

Brings up the Enter Passwords screen for you to input the passphrase you will use to restrict access to a Keyfile.

See the "**2nd User Access**" entries in the "**How To** " section, for usage instructions.

### **CLEAR ALL PASSWORDS CACHED IN DRIVER ETC:**

Clears any passphrase held in memory by both the VxD component and the ScramDisk interface.

N.B. If the "**Enter all passwords in low level RED message mode**" setting is enabled then both the first two menu items will use this rather than the standard windows password screens.

## Partitions



### **REMOUNT/REFRESH:**

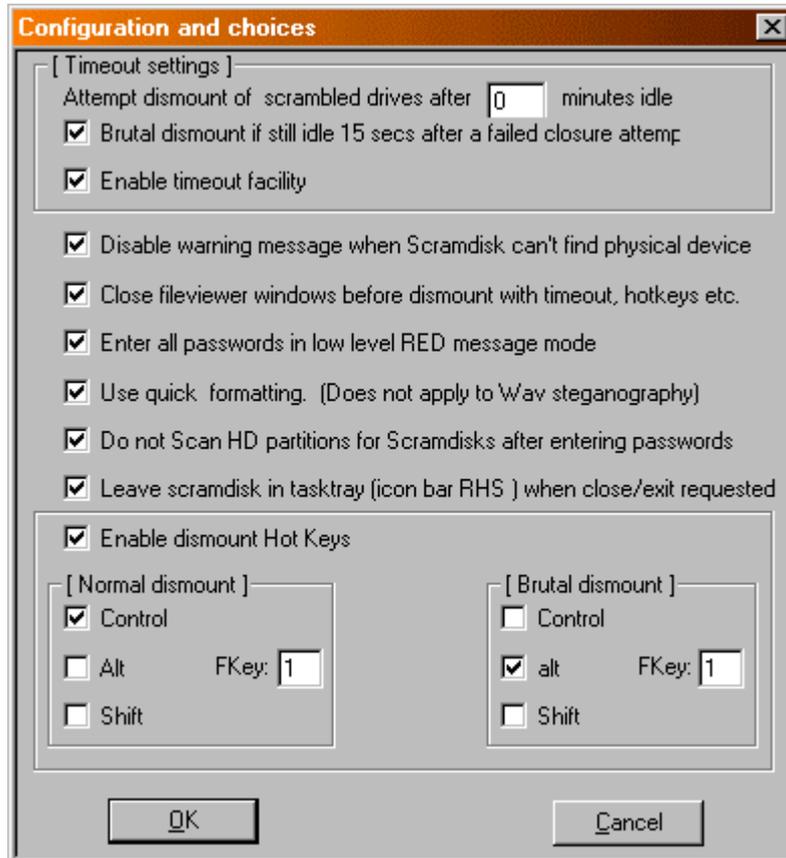
Updates the Device / Partition window and causes ScramDisk to attempt to mount any Encrypted Partitions for which it has a cached passphrase.

## Timeout/Configure



### **TIMEOUT AND OTHER SETUPS :**

Invokes the dialogue for configuring the timeout feature and other settings.



See the "How To " sections on:

"Using the timeout feature" for a description of the majority of these settings.

"Creating an encrypted volume" for the use of the "Use quick formatting (Does not apply to Wav steganography)" setting.

See the "Screen Descriptions and Menus" section on "The RED Low Level Message Screen" for an explanation of the effect of the "Enter all passwords in low level RED message mode" setting.

### **DISABLE WARNINGS WHEN SCRAMDISK CAN T FIND PHYSICAL DRIVE:**

Usually ScramDisk warns you that the physical media type cannot be verified, which is not a problem if the disk resides on a normal, local, hard drive. If the ScramDisk volume being mounted resides on a network drive or on removable media then ScramDisk issues a warning. This option disables the warning and was added at the request of several users.

**DO NOT SCAN HD PARTITIONS FOR SCRAMDISKS AFTER ENTERING PASSWORDS:**

Tells ScramDisk not to perform a scan of hard disk partitions when you enter a new passphrase.

**LEAVE SCRAMDISK IN TASKTRAY (ICON BAR RHS) WHEN CLOSE/EXIT REQUESTED:**

Causes ScramDisk to remain as an icon in the Systray after it has been closed.

## Wipe



### FREE SPACE:

Causes ScramDisk to write random data to all free space on the disk. This prevents the acquisition of data from the remains of deleted files.

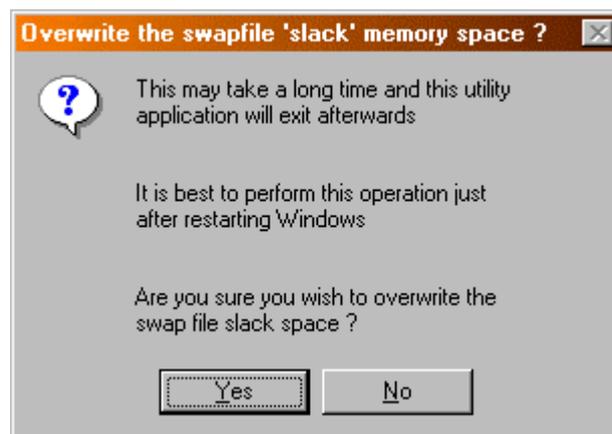


You can specify the drive you want ScramDisk to wipe the free space on and the number of times it is to repeat the operation (i.e. passes).

Free space usually still holds the data that was there when the files it previously constituted were deleted.

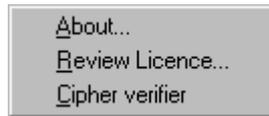
Wiping free space securely erases previously deleted files such that they cannot be restored by Undelete or by a disk sector editor.

### OVERWRITE SWAPFILE SLACK:



Any slack left when the swapfile contracts may contain data, overwriting the slack securely clears any data in it.

## About



### **ABOUT:**

Credits and Version information.

### **REVIEW LICENCE:**

An opportunity to look over and re-confirm or refuse the licence you agreed to by using this software.

### **CIPHER VERIFIER:**

Invokes a utility that allows you to verify that the algorithms used by ScramDisk produce the same ciphertext as 'known good' implementations published elsewhere.

See the 'How To... Verify the algorithms used' section for usage.

# Technical Overview

## ***The Encryption Process***

The process of creating an encrypted disk is independent of the algorithm chosen. All disk containers are created in the following manner. When mounting a disk (assume one algorithm is only available) the procedure is:

1. The first 2048 bytes of the container are read into a buffer.
2. The user's password (up to 160 text bytes and assuming the correct one) is passed to SHA-1 for hashing to a digest value.
3. The chosen cipher algorithm is initialised with the key from the digest of SHA-1 obtained in (2)
4. The 2048 bytes in the buffer read in (1) are then decrypted with the chosen algorithm initialised with the digest value.
5. The MASTER KEY data (up to 256 bits) stored in the buffer+1024 is retrieved. This value has been decrypted in stage (4) along with the other data.
6. The chosen cipher algorithm is reinitialised with the correct length of bits as retrieved in (5) (256 for blowfish etc.....) This is the same key that is now used to decrypt the whole of the disk.
7. Two sectors which were filled with identical but random data (encrypted with the MASTER KEY at format time as are all data areas) are read, and decrypted with the master key, and IVs etc.
8. If these two sectors now produce identical data, the KEY/ IVs can be assumed to be correct, and windows is called to initialise the disk. Otherwise the driver returns without doing anything more.
9. If all is well Windows sees a new disk, all access which will go through the sd.VxD code via DCBs for the new device. The "Calldowns" in the DCBs call the correct code to decipher all the relevant sectors etc.

So, to summarise: Your passphrase is hashed with SHA-1 which unlocks 2 areas on the disk. An area containing the random values to be used for IV's and pre-whitening<sup>1</sup>. Another totally separate section that contains the key to be used for the encryption and decryption of the sectors on the disk. This key is then used as the key in the conventional encryption algorithm. The same key is used for all sectors on the disk, which doesn't matter as a different IV is used for each sector.

The two areas of random data are in no way related.

---

<sup>1</sup> As per pg 366 Applied Cryptography 2<sup>nd</sup> Ed

## Supported Encryption Algorithms

ScramDisk supports a number of algorithms in the first release. All Algorithms are used in CBC mode using a random value as the IV. Additionally, another random value is used to obfuscate the link between the plaintext and ciphertext (this process is called 'pre-whitening'). The algorithms are as follows:

- **3DES.** This is far better than DES; it uses 3 applications of the DES cipher in EDE (Encipher-Decipher-Encipher) mode with totally independent keys. Outer-CBC is used. This algorithm is thought to be very secure (major banks use it to protect very valuable transactions) but it is also very, very slow.
- **Blowfish.** This is a high security encryption algorithm designed by Bruce Schneier the author of Applied Cryptography and owner of the company Counterpane. This algorithm is very fast, is considered secure and is resistant to linear and differential analysis. This is my personal cipher of choice.
- **DES.** This is the Data Encryption Standard algorithm designed in the early 1970's by IBM (with input from the NSA). It is OK, but a single key can be broken in 3 days by a poorly funded organisation (the EFF!) ☹. This algorithm was provided for completeness, but it is quite slow and considered weak.
- **IDEA.** This is a cipher produced by Xuejia Lai & James Massey. It is fairly fast and is considered secure. It is also resistant to both linear and differential analysis. To use this cipher in anything other than personal use you need to pay a royalty to Ascom. See the license details later in this document for information on royalties.
- **MISTY1.** This is an algorithm designed by M. Matsui of Mitsubishi. It is a reasonably fast cipher that is resistant to both linear and differential analysis. It is fairly new though, so use it with caution.
- **Square.** Square is a very fast and reasonably secure block cipher produced by John Daemen and Vincent Rijmen. It hasn't been subject to as much peer review as Blowfish, 3DES, IDEA etc. so may be susceptible to attacks.
- **Summer.** This is a proprietary stream cipher constructed by the author. It is designed for speed alone. It is supplied in the program for backward compatibility with version 1 of ScramDisk and is not recommended for use on newly created disks. Instead use TEA or Blowfish, which are both reasonably fast.
- **TEA.** Tiny Encryption Algorithm is a very fast and moderately secure cipher produced by David Wheeler and Roger Needham of Cambridge Computer Laboratory. There is a known weakness in the key schedule so it is not recommended if security is the prime consideration. TEA is provided in two forms, 16 & 32 rounds. 32-rounds are obviously more secure than 16, but also slower.

## Algorithm Summary

The following table details the performance of the different algorithms:

<b>Algorithm</b>	<b>Author</b>	<b>Implementation</b>	<b>Block Size (bits)</b>	<b>Key Size (bits)</b>	<b>Speed (m:s)</b>
3DES (3-key, EDE)	Diffie & Hellman	Assembler	64	168	4:05
Blowfish	B.Schneier	C	64	256	0:55
DES	IBM & NSA	Assembler	64	56	1:42
IDEA	Xuejia Lai & J.Massey	Assembler	64	128	1:07
MISTY1	M. Matsui	C	64	128	2:50
Square	J.Daemon & V.Rijmen	Optimised C	128	128	0:39
Summer (Stream)	Aman	Assembler	N/A	128	0:31
TEA (16 Rounds)	D.Wheeler & R.Needham	Assembler	64	128	0:46
TEA (32 Rounds)	D.Wheeler & R.Needham	Assembler	64	128	1:03

The column 'Speed' gives relative performance figures for all of the ciphers. The times are based upon copying a 50Mb file from a normal disk to a ScramDisk disk on a Pentium 166mhz. Copying the same file from disk to disk (e.g. not to an enciphered volume but just disk to disk) took 28 seconds.

## Frequently Asked Questions (FAQ)

### ***Q: What can I store on my computer with ScramDisk?***

A: Anything you can store on any other Windows disk, apart from ScramDisk file images. They cannot be recursively stored on other ScramDisk disks. Otherwise programs, data, anything.

### ***Q: What cipher is best?***

A: I don't know! 3DES is thought to be extremely strong, but may be too slow to use for all ciphered disks. IDEA and Blowfish are good choices – they are both thought to be secure against all known attacks. I personally like Blowfish because of its larger key size, very reasonable speed and lack of licensing issues. Summer is thought to be weak. TEA, Square & MISTY1 are OK but are all relatively new. DES is certainly weak against a determined adversary.

### ***Q: What is that horrible "red screen" into which I have to type passwords?***

A: This screen is a *very* low-level mechanism provided in Windows 95 that is usually used for critical error messages. By entering a password into this screen, rather than a conventional password dialog box, you prevent certain "sniffing" programs like Skin98 from being able to read the keystrokes that make up your passphrase.

### ***Q: What kind of "disk" does Windows see on a ScramDisk disk?***

A: Windows "sees" a standard FAT 16 disk in all cases. The data may actually be stored in a partition, or on a file on FAT32, or FAT16, in a CD FILE on CDFS, even at the other end of a network.

### ***Q: If I create a virtual disk with ScramDisk, can I defrag it, and repair it like other FAT disks?***

A: Defrag can be run on a "Scramdisk" disk just as it can be run on any standard disk. Scandisk can be run to repair any possible faulty DOS structure, just as a standard disk. Indeed the system doesn't know it isn't a standard disk!

### ***Q: What about FAT32 support?***

A: There is limited support for FAT32 in ScramDisk, it is possible to create a ScramDisk volume file on a FAT32 disk but it is not possible to create a FAT32 volume. All ScramDisk containers currently have to be formatted with the FAT16 file system – this restricts ScramDisk volumes to a maximum of 2Gb in size.

### ***Q: Where are the passwords stored on the disk?***

A: They are not. The disk is mounted statistically, not by comparing passwords. There are two sectors with the same (randomly derived data) having different sector keys. The data on these sectors with an incorrect password look different. Only when the correct password is supplied, creating the correct pair of keys (one for each sector) will the two sectors show the same data, and the passwords be assumed correct.

### ***Q: Can anyone see the file names I've stored on the disk, when it is inaccessible?***

A: No. The boot sector, directories, File Allocation Tables, and data are all scrambled using the algorithm of your choice.

### ***Q: How do I back up my files, stored on ScramDisk disks?***

A: Just as you usually would. However, if they are to remain secure, you will need to back them up on to a second ScramDisk drive. Just open both drives, and drag and drop the files, in windows from one to the other. Another option is to backup the entire encrypted volume.

### ***Q: ScramDisk doesn't work with x?***

A: ScramDisk *should* work with all applications, but there are issues with some applications, for example JBN. 9 times out of 10, users who report problems with ScramDisk are actually doing something wrong, for example:

1. Trying to create too many files in the root directory of a drive.
2. Trying to do something with a read only file.

Obviously, these errors can occur on any type of disk. Please report any application issues to the author.

**Q: Does ScramDisk work with DOS ?**

A: ScramDisk is a Windows VxD driver system, with a Win32 utility application. It will work perfectly well within a DOS prompt under Windows, and allows the use of DOS utilities to access its disk in the normal way, but of course, it won't work unless Windows 95 is the underlying operating system. There is a DOS version of ScramDisk, but only one which will read ScramDisk partitions rather than file hosts.

**Q: Do I have to have the "Scramdisk.exe" utility program running on the desktop when I am using my ScramDisk disks?**

A: No. The VxD driver "SD.vxd" installed in the "..\system\iosubsys" directory does all the horsework. Unless you wish to close disks or open new ones, you can quit the utility program, when you have finished with it.

**Q: Why doesn't it work on Windows NT?**

A: Windows NT uses a completely different driver model, called the Kernel Mode Driver (KMD) which requires a different knowledge base to program. Windows 95/98 uses "VxDs" and the "IOS" for disk drivers. The two are completely different, and incompatible. Hopefully some kind soul will help the cause and help produce an NT version. The new Windows Driver Model that comes with NT v5 & Windows 98 will not help either, as this only covers display & multimedia drivers.

**Q: What if I forget my passphrase?**

A: Assume that you have lost your data! It would not be a very secure system if I could tell you how to get it back, would it?

**Q: What makes a good passphrase?**

A: Several pieces of advice can be given to users who have the task of choosing a passphrase:

1. Make the passphrase as long as possible. The passphrase can have 39 characters per line and there are 4 lines – so a passphrase can be up to 156 characters.
2. Try and make use of both upper and lower case letters.
3. Include both numbers and punctuation characters, such as ; : , . ! " £ etc
4. Try not to pick a single word or a well-known piece of literature – this will enable a dictionary attack on the system.

With ScramDisk, mounting a dictionary attack is a very time consuming task – for each password that is unsuccessfully tried the following is necessary: 2xSHA-1 followed by 1xinitialisation and 1xblock decipher **for each algorithm** – this is because the algorithm used to encipher the disk is not stored.

**Q: Help! Parts of my passphrase appear in the enciphered volume!?**

A: Statistically this is to be expected. For example, if you create a 100 Mb enciphered volume then it is expected that each 3 character combination (e.g. AAA, AAB, AAC etc) will appear approximately 16

times:  $(100*1024*1024)/256^3$ . Thus the users passphrase will most likely appear in the enciphered volume in 3 letter blocks.

This occurs because encrypted data looks like random numbers - it would be possible for ScramDisk to check and ensure that parts of the passphrase do not occur – but this would enable analysis. Since  $(16*1024*1024)/256^3 = 1$ , you would expect, on average, to see every possible 3 character combination in a 16Mb file.

Do be concerned if 5 letter chunks of your passphrase occur in the volume though – the chances of this happening accidentally are extremely small.

***Q: How can every disk I create look different, even if I create the disk using the same password and algorithm and put the same data in it?***

A: You will never generate the same master key table. The chances of doing so are astronomically remote. It is this master key table that is scrambled with your password and the unscrambled table which (un)scrambles the data on your disk. No two master key tables are alike -unless you copy a ScramDisk host file elsewhere.

***Q: Is there anything I should not do?***

A: Don't copy ScramDisk host files (ones which "contain" a ScramDisk disk) and then start to use them separately. For each new disk you wish to create, you should use the creation facilities/partition formatter provided in the utility program. This ensures greater security. If you did copy a host file and continue to use it then both drives would operate with the same IV's and pre-whitening values (because they have the same random data at the start of the disk), which could aid cryptanalysis.

***Q: Why was the program produced?***

A: Why was PGP produced? Why not? If we honestly believed that strong cryptography was going to cost lives or threaten national security, we would have been morally and ethically obliged not to develop or release the package. But the truth is, there has not been a convincing argument from any political or lawmaking group as to why strong cryptography shouldn't be produced, used, distributed and sold.

I personally like the 'keys' analogy. We don't have to give the Government copies of our home and work door keys, so why should we afford them the same privilege with the keys to our data? The police are welcome to access my data with a valid court order in the same way that they can enter my house with a valid search warrant.

I also like Phil Zimmerman's 'postcard' argument. When people send letters they use envelopes to ensure a level of security, they don't send letters without envelopes because they don't have to. Sending letters within an envelope is considered acceptable because everyone does it. Everyone should have the right to use strong crypto.

The real reason the American (and UK?) government are opposed to strong-crypto is that they are provided with far too much intelligence from monitoring communications to allow the proliferation of strong crypto, which would make there job necessarily harder. Read Puzzle Palace / For the President's Eyes Only if you don't believe me!

Both myself and the Author of the program are IT professionals without criminal records (not even driving endorsements!). We are neither "law breakers" nor "anarchists" - we just believe that privacy should be a right and that strong cryptography should be accessible to anybody who wants it.

***Q: Is there any other similar software for Win95?***

A: Yes. Jettico's Bestcrypt, and PGP's PGPDisk for windows 95. They are of course incompatible with each other, and use different scrambling algorithms. BestCrypt uses Blowfish / GOST/ DES, PGPDisk uses CAST. ScramDisk (being free) is the cheapest. Currently, neither of the programs are supplied with source code – so you have to trust the authors implementation.

**Q: Are there in “international” issues?**

A: Just the one: the low-level Red Screen should be avoided if you are using anything other than a QWERTY keyboard.

This user manual is currently being converted to French & Russian.

**Q: Why does an explorer window appear when I mount a ScramDisk volume? Can I disable this functionality?**

A: This “feature” is provided for two reasons:

1. Without calling an Explorer window showing the new drive, applications and other Explorer windows will not be updated to reflect the new drive – this is confusing for many users.
2. Windows 95/98 is inconsistent – even without calling the Explorer window, *sometimes* one is created automatically by the operating system. The author decided that it was best to make the operation consistent.

Currently, it is not possible to disable this functionality.

**Q: Why does ScramDisk include so many ciphers?**

A: When the program was first announced, several users criticised the program because it contains too many algorithms for three main reasons:

1. Having a large number of algorithms to choose from may confuse users.
2. It would be better to have a program that implements a few algorithms and works rather than implement loads of algorithms and is flakier.
3. No security is afforded by offering more than one algorithm.

Both the author and myself believe there are good arguments for having plenty of algorithms:

1. The default option of Blowfish is provided which is a fast and secure block cipher with no known attacks better than brute force despite having been fairly extensively cryptanalysed. If users don't know about all the different algorithms then this is a reasonable default choice.
2. All algorithms have been implemented using well-known code from the web, rather than being completely rewritten. It is highly unlikely that any of the code is defective, as all ciphers have been checked against the Test Vectors freely available on the web. Users can check Test Vectors for themselves using a mechanism built into the program.
3. Even if a defective algorithm were added to the program, it would only cause the program to act improperly when this algorithm is chosen. The security of the system as a whole will not be compromised, only disks created with the algorithm.
4. We believe that security is certainly added by including multiple ciphers. Nowhere on the virtual disk is a record of which algorithm is used to encrypt the disk. Thus someone who wishes to 'crack' an encrypted disk will have to first determine which algorithm is used. Generally, encrypted data looks like random numbers, so doing this is not a trivial task!
5. In response to point 3 above; if the program were to be supplied with one built in cipher and it was later discovered that this cipher was weak then all users of the program would have encrypted disks that are also weak. This would mean that the program would be useless until someone added another cipher! Users of ScramDisk can choose whichever algorithm they

have most faith in. The author thought it improper to dictate to all users which algorithm they can use. At least now they have a reasonable choice. Really, the choice of algorithm can be seen as part of the key.

6. No algorithm is perfect for all situations; some data may just need 'low-security' encryption that is not noticeably slower than no encryption whereas some situations require a very high level of security. 3DES is arguably the most secure cipher, but is very slow, TEA however is the opposite; it is extremely fast, but may not be secure against a well funded adversary.
7. If users have read the above, and still believe that they wish to have ScramDisk with one cipher, there is nothing to stop them from removing all the other ciphers and recompiling the program.

**Q: What backdoors exist in ScramDisk?**

A: To the best of our knowledge, none. We have no motivation to produce a defective program, so draw your own conclusions. Oh, and inspect the source code if you are so inclined!

ScramDisk is not totally secure (and nor is any security program!). There are a number of ways an attacker may try infiltrating your system:

1. Look for applications that leak data. A very well known word processor has an interesting bug that leaks the parts of the raw contents of the disk when saving an OLE Compound Document.
2. Look for data that isn't deleted securely. Ok, everyone knows that you can undelete a file easily. Did you know that even a file that has been 'wiped' can potentially be recovered by looking at the surface of the disk. Deleted files should be securely wiped using an appropriate program (PGP v6 contains a secure file-wiping program – users of PGP v5.x should be aware that the file wipe functionality is possibly insecure).
3. Look for data that has leaked in other ways. Temporary files and the swap file spring to mind. These both need to be securely erased too.
4. Using a "Tempest" type attack. Basically, electrical emissions from the monitor, hard drive and even keyboard can be detected and recorded from a distance away. This may allow an eavesdropper to see what is on your screen or detect your pass-phrase as you type it.
5. Brute Forcing. This can happen in a number of ways: they can try brute-forcing your pass-phrase or they can try to brute force the algorithm. To thwart the first attack it is important to use a large pass-phrase that isn't easily guessed, it helps to use both upper and lower case and numbers as well. This is hard work (and will take around  $2^{127}$  operations with most of the ciphers included with ScramDisk - DES & Summer are exceptions).
6. Some of the ciphers included may be susceptible to attacks not known about in public. The NSA/GCHQ *may* have a mechanism faster than brute-force of attacking the algorithms. We have not included any weak algorithms in the original distribution (apart from Summer, which is included for backwards compatibility), but who can tell what the Intelligence Agencies can do with Blowfish, IDEA, 3DES et al?
7. Install an amended version of ScramDisk on your computer that secretly stores your pass-phrase so that a CIA agent can later read it. (Or use a program like SKIn98 to do it!) Far fetched? Possibly, but you should be aware that this kind of attack exists. There is no real way to defend this attack. Check the PGP Signatures of the ScramDisk files against the executables on your computer, but could your copy of PGP have also been amended?
8. Beating you until you spill your pass-phrase. Truth drugs also work, apparently.

The author has done as much as he can; giving you a program which offers ciphers that are believed to be strong, contains no key recovery mechanisms, is distributed with source code so you can independently verify the operation of the program and offers PGP Signature files so that you can check the authenticity and integrity of the package. The rest is up to you!

## Program Rationale

This section aims to detail why ScramDisk works the way that it does.

### ***Q: Why do you type the passwords in first?***

A: So they can be used again and so any hard disk partitions that use them, will be opened. Once a password is entered, it can be used for all disks that were formatted with it, until you clear the password cache (in the application) or type more than 8 in. In that case it goes off the end of the password list.

### ***Q: Why can't you double-click on a ScramDisk host file to start the mount the disk?***

A: Any type of file can be used as a host file. This is deliberate; it makes ScramDisk volumes harder to spot.

It may be noticed that as little use of possible is made of the system registry and file types. This is deliberate. It is not necessary to register the software with the system, so it can be removed almost without trace if required. The win32app Scramdisk.exe can even be contained on a floppy disk drive if need be. The driver "sd.vxd" has to reside in system\iosubsys directory; there is no alternative. But that can be simply removed.

Certain possibilities have to be cast aside, if the use of the system registry is to be avoided. One of these is to be able to click on a cabinet file, and run the app. Future versions will allow you to set up the file extension and association yourselves. In the meantime, you'll have to be satisfied with BROWSE and "Drag and Drop" from the Scramdisk.exe application.

### ***Q: Why don't you get an error, when your passwords are incorrect?***

A: To give an error, would make it obvious the file was indeed a scrambled file (rather than a file full of junk, and in the case of WAV, an untouched music file). The fact that files are untyped, and all possible ciphers have to be "tried" against them, means that errors are meaningless. ScramDisk does not know the file isn't a valid file. It only knows when it has valid passwords, and other data, to convert bytes into their correct values, which then give us a win95 disk!

### ***Q: Why can't you change your passwords?***

A: From v2.02 onwards it **is** possible to change the password associated with a volume. This, unfortunately, still doesn't completely re-encipher the disk – it only re-enciphers the key area at the start of the disk. Totally re-enciphering the disk can be problematic in the event of power failures.

### ***Q: Why does a key disk file not open new disks I format with the same password?***

A: Key disks were designed to allow others to access *particular* disks, whilst keeping your passwords secret. The data in a key disk file, contains information to decode those absolutely unique disks that were mounted on ScramDisk, when the key disk was created. The data on the key disk file is enciphered "as if" the key disk password was used when the disk was formatted. Your own access password is never involved when a ScramDisk is opened with a key disk.

## Future Developments

ScramDisk is a work in progress. Version 2 is the first version to be released in the public domain. It is hoped that people from around the world will help to further develop ScramDisk. The author and myself have highlighted a number of areas for future development. They are listed in order of importance, with the most important item first:

- 1) Make the user interface easier to use. Possibly provide command line tools to mount / dismount drives etc, allow the program to associate itself with a file extension (.SVL?) if the user wishes.
- 2) Develop a version of ScramDisk for Windows NT.
- 3) Change the architecture so it is more standard and modular. The program ignores some C conventions, which I believe can be easily rectified. Also it needs to be altered so it is easier to add new ciphers and hash algorithms.
- 4) Add additional ciphers. This program already has a fair number of well-respected ciphers, but we would like to see more added. Why? See the FAQ section for details..... We are particularly keen to see the very good-looking AES candidates added, namely MARS, RC6, TwoFish, CAST-256, Safer+ and Serpent. Other ciphers thought worthy of inclusion are GOST, RC5, 3-way, and Luby-Rackoff using SHA-1. ScramDisk works best with algorithms with the following characteristics:
  - i) Slow key-initialisation but fast encryption speed (in preference to quick initialisation and slow encryption speed).
  - ii) A low amount of key-dependant data. This data has to be reserved in non-swappable kernel memory, so the smaller the better.
- 5) Add additional hash algorithms. Currently the system only supports SHA-1 which is OK, but should a major weakness be found, the whole program will be useless and all disks created with ScramDisk may be compromised. RIPE-MD160 is probably a good choice or one of the constructs based upon a block encryption algorithm, like Abreast Davies-Mayer.
- 6) Add proper steganography support (like Ross Anderson's Steganographic File System).
- 7) Possibly change the source of random data from Summer to Yarrow, a Counterpane random number algorithm.
- 8) Change the implementation of Blowfish, Misty1, Square & SHA-1 from straight C to assembly language, or at least use an optimised C version.
- 9) Add the enhanced version of TEA (called TEAX) which solves the key schedule problem. This will probably need to be added alongside the existing implementation to provide backward compatibility.

If you are interested in further developing the program, either in one of the areas listed above or in another direction, please contact us. We are very keen to co-ordinate the development effort to ensure that each build is free from bugs and, as far as possible, is compatible with other versions. We would also like to keep a definitive version of the program on the web-site (along with any other release builds).

*Maybe developing ScramDisk further would make an interesting under-graduate final year project?*

## Program Revisions

This section has two purposes; It outlines the various versions of ScramDisk that are in circulation and also lists some known problems that are to be / have been solved.

### Program Versions

Version	Release Date	Details Of Release
V2.02c	20 <sup>th</sup> Sept 98	Fixes several bugs: Quick Format under 98, recursive password box problem, "freeze" in Explorer problem. The documentation has been corrected in several areas and is also now available in Adobe Acrobat format.
V2.02	24 <sup>th</sup> August 98	<p>Solves the following bugs: BestCrypt, Window Fonts, Log off / log on bug, SKF bug, Intermittent freezing bug (caused by buffer misallocation). Enhancements include:</p> <ul style="list-style-type: none"> <li>• Can now have 8 mounted volumes rather than 4.</li> <li>• Very low level (Red) password entry screen that stops SKIN98 etc. snooping key-presses.</li> <li>• 16 (NORMAL) devices can be displayed rather than 8.</li> <li>• Shows last opened time &amp; date of an enciphered volume.</li> <li>• Minor changes to Cipher Verification form.</li> <li>• Now allows forced dismount of drives.</li> <li>• Option to minimise to system tray.</li> <li>• Option to disable "No physical" warning message. (For Bear)</li> <li>• Hotkeys for dismount and brutal dismount.</li> <li>• Some command line options have been added. (To Mount container / dismount/ dismount brutal).</li> <li>• Can now change the passphrase used to access a disk (though this doesn't re-encipher the disk).</li> <li>• Now possible to revoke SKF access.</li> <li>• Completely rewritten User Manual.</li> <li>• Now comes with a small example app that demonstrates mounting disks programmatically.</li> <li>• Option to disable "No physical" warning message. (For "Bear").</li> </ul>
V2.01	21 <sup>st</sup> July 98	An interim build of ScramDisk that solved the BestCrypt bug. Not widely distributed.
V2.00	14 <sup>th</sup> July 98	<p>The first release given to the public. Contains the following ciphers: 3DES, Blowfish, DES, IDEA, Misty1, Square, Summer, TEA (16 &amp; 32).</p> <p>SHA-1 is the sole hash algorithm and the program supports 8 &amp; 4 bit WAV steganography. This version now works under '98.</p>
V1.00	20 <sup>th</sup> Nov 97	First release. Contains only the proprietary cipher 'Summer'. This was not publicly released.

## Bugs

The following 'bugs' have been found and will be fixed in due course. To report new bugs send an e-mail address to Sam Simpson at the address given in the 'Contacting the author' section.

<b>Problem</b>	<b>Date noticed</b>	<b>Resolved in version</b>
Quick format may not function correctly under Windows 98.	13 <sup>th</sup> Sept 98	V2.02c
Intermittent freezing when clicking on Explorer windows.	5 <sup>th</sup> Sept 98	V2.02c
Password dialog box keeps appearing, even when cancel pressed.	3 <sup>rd</sup> Sept 98	V2.02c
When users log off then back on again (e.g. without shutting down) ScramDisk may refuse to load.	18 <sup>th</sup> Aug 98	V2.02
Document rather than folder icon in main display window.	24 <sup>th</sup> July 98	V2.02
Timeout doesn't work in some circumstances when the ScramDisk executable isn't loaded.	19 <sup>th</sup> July 98	V2.02
Program locks computer totally when trying to mount a ScramDisk disk when there are no drive letters available.	17 <sup>th</sup> July 98	N/A
IE4 (and thus Windows 98) has some problems with redraws in Tree Views.	11 <sup>th</sup> July 98	V2.02
BestCrypt and ScramDisk don't coexist perfectly. To do with BestCrypt creating lots of ports that ScramDisk thinks are real hard disks.	21 <sup>st</sup> June 98	V2.02
Intermittent freezing bug – caused by buffer misallocation.	20 <sup>th</sup> June 98	V2.02
The fonts under the drives don't appear properly when Large fonts are used.	20 <sup>th</sup> June 98	V2.02
Failure to open WAV files, later in a windows session, means your machine cannot allocate the locked buffer needed. No error is given, just failure to access your WAV based disk. The buffer is only (permanently) allocated when a WAV file is first used. Mount the WAV early in the Windows session to avoid this. Future versions will give an error and/or have an option to claim the buffer at system start-up. Normal ScramDisk container files and partitions are not affected.	20 <sup>th</sup> June 98	V2.02

## License Details

ScramDisk can only be used if you agree with the following terms and conditions:

1. You accept the creator of this software cannot be responsible for **any** loss of data however caused (including by any incorrect operation of this software program despite 'best efforts') and you agree to back up any files that you consider important before you use this software on your system.
2. You agree the creator of this program is anonymous, but wishes to retain copyright and commercial rights to this software.
3. You agree not to redistribute this software in any form other than that in which it was received by you, and will include all files exactly as present when it was so received, if you do distribute it.
4. You agree in the event of loss, or forgetting of passwords used by this software, no technical support can be given to assist in recovery such passwords. Forgetting any passwords, EQUATES to loss of your data when that data is stored on any disk partitions, or disk drive images created, and opened by the execution of this software. You accept no back doors exist, to gain access to scrambled data.
5. You agree that some of the ciphers used are the intellectual property of others, and may need a licence for commercial use, such as use on a business system. You acknowledge this is especially true in the case of the IDEA algorithm and will read the documents regarding the Ascom conditions of use of IDEA, which can be found at the bottom of this page.
6. You agree that if you obtain the publicly available source code, and amend it you will submit the amended program and new source code to the originators for publication, and understand that these amendments shall not violate compatibility with older versions of the software or reduce security levels in any way.

### ***IDEA Conditions of use and required notice:***

This Software/Hardware product contains the algorithm IDEA as described and claimed in US Patent No. 5,214,703, EPO Patent No. 0482154 and filed Japanese Patent Application No. 508119/1991 "Device for the conversion of a digital block and use of same" (hereinafter referred to as "Algorithm").

Any use of the Algorithm for Commercial Purposes is thus subject to a license from Ascom Systec Ltd. of CH-5506 Mägenwil (Switzerland), being the patentee and sole owner of all rights, including the term IDEA.

Commercial Purposes shall mean any revenue generating purpose including but not limited to:

- i) using the Algorithm for company internal purposes (subject to a Site License).
- ii) incorporating an application software containing the Algorithm into any hardware and/or software and distributing such hardware and/or software and/or providing services related thereto to others subject to a Product License).
- iii) using a product containing an application software that uses the Algorithm (subject to an End-User License), except in case where such End-User has acquired an implied license by purchasing the said product from an authorised licensee or where the End-User has already signed up for a Site License.

All such commercial license agreements are available exclusively from Ascom Systec Ltd. and may be requested via the Internet World Wide Web at <http://www.ascom.ch/systec> or by sending an electronic mail to [IDEA@ascom.ch](mailto:IDEA@ascom.ch). Any misuse will be prosecuted.

Use other than for Commercial Purposes is strictly limited to data transfer between private individuals and not serving Commercial Purposes. The use by government agencies, non-profit organisations etc. is considered as use for Commercial Purposes but may be subject to special conditions. Requests for waivers for non-commercial use (e.g. by software developers) are welcome.

## Resources

See the ScramDisk web page for a link of Web links to interesting sites covering cryptography and information security. Anyway, I highly recommend the following books:

### ***Cryptography and Information Security***

**Applied Cryptography - 2nd Edition**, B.Schneier, 1996.

ISBN: 0-471-11709-9

Crypto-bible for crypto-wannabies and professionals alike. THE definitive piece, need I say more?

**Handbook of Applied Cryptography**, Menzes et al, 1996.

ISBN: 0-8493-8523-7

Heavy and comprehensive!

**Cryptography and Data Security**, D.Denning, 1983.

ISBN: 0-201-10150-5

Sound cryptography introduction.

**Security in Computing - 2nd Edition**, C.Pfleeger, 1997.

ISBN: 0-13-185794-0

Covers both cryptography and the wider issues of information & computer systems.

**Computer Security Handbook - 3rd Edition**, Hutt, Bosworth & Hoyt, 1995.

ISBN: 0-471-11854-0

The Security Officers bible. A very serious tomb!

**Cryptography and Secure Communication**, M.Rhee, 1994.

ISBN: 0-07-112502-7

Nuts and bolts cryptography.

**E-Mail Security with PGP and PEM**, B.Schneier, 1995.

ISBN: 0-47-105318-x

The title says it all.

### ***Wider Issues***

**Privacy on the Line - The Politics of Wiretapping and Encryption**, W.Diffie & S.Landau, 1998.

ISBN: 0-262-04167-7

Excellent, balanced discussion of the national security/law enforcement vs. personal privacy debate.

**The Code-Breakers**, D.Kahn, 1996.

ISBN: 0-684-83130-9

"The Comprehensive History of Secret Communications from Ancient Times to the Internet". It is!

**The Puzzle Palace**, J.Bamford, 1983.

ISBN: 0-14-006748-5

America's most secret agency revealed. Fascinating! Who only knows how much they have progressed in the 15 years proceeding this publication?

**For the President's Eyes Only**, C.Andrew, 1996.

ISBN: 0-06-092178-1

Not a book about Ms Lewinsky but rather "Secret Intelligence and the American Presidency from Washington to Bush". A great insight into intelligent agencies in the USA.

**Marching Orders - The Untold Story of World War II**, B.Lee, 1995.

ISBN: 0-517-57576-0

Discusses the use of ULTRA & MAGIC by the allies.

**Inside CIA s private world**, H.B.Westerfield, 1995.

ISBN: 0-300-07264-3

Recently declassified articles from the CIA's *Studies in intelligence*. Interesting!

**Betrayal The Story Of Aldrich Ames An American Spy**, Weiner, Johnston & Lewis, 1995.

ISBN: 1-86066-046-0

Who was more incompetent? Ames or the CIA?

**A Century Of Spies Intelligence in the Twentieth Century**, J.T.Richelson, 1995.

ISBN: 0-19-511390-x

ok, if a little light-weight.

**The US Intelligence Community**, J.T.Richelson, 1995.

ISBN: 0-8133-2376-2

"The authoritative survey of the American cloak-and-dagger establishment". Indeed!

**Persuasion and Privacy in Cyberspace**, L.Gurak, 1997.

ISBN: 0-300-06963-4

Haven't read it yet.

**Technology and Privacy: The New Landscape**, P.Agre & M.Rotenberg, 1997.

ISBN: 0-262-01162-x

Haven't read it yet.

**Shamans, Software and Spleens**, J.Boyle, 1996.

ISBN: 0-674-80522-4

Haven't read it yet.

**The Art of Computer Programming Volume 2 Seminumerical Algorithms**, D.Knuth, 1998.

ISBN: 0-201-89684-2

Loads of details on semirandom number generation, fast exponentiation etc.

**The Right To Privacy**, E.Alderman & C.Kennedy, 1995.

ISBN: 0-679-41986-1

Haven't read it yet.

## Great Crypto & Info Security Quotes

*"The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated..."*

-- The Fourth Amendment to the U.S. Constitution

*"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."*

-- The First Amendment to the U.S. Constitution

*"The freedom of speech and of the press guaranteed by the Constitution embraces at the least the liberty to discuss publicly and truthfully all matters of public concern without previous restraint or fear of subsequent punishment."*

-- Roth v. United States, 354 U.S. 476 (1957)

*"...domestic intelligence activities [that] threaten to undermine our democratic society and fundamentally alter its nature"*

-- Senate Church Committee report, 1976

*"the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis"*

-- A Congress requested National Research Council report "Cryptography's role in securing the information society", 1996

*"on balance, the advantages of more widespread use of cryptography outweigh the disadvantages"*

-- ibid

*"The FBI, on the other hand, stretched the truth and distorted the fact. It seems fair to conclude that the government has not made its case regarding encryption."*

-- Diffie in "Privacy on the line", 1998 - explaining how intelligence agencies (mis)use wiretap statistics.

*"In total, therefore, the U.S. economy will lose between \$35.16 and \$95.92 billion over the next five years, as a consequence of current administration policy [on crypto]."*

-- Economic Strategy Institute report "Finding the Key", 1998

*"The right to be let alone is indeed the beginning of all freedom."*

-- Supreme Court Justice William O. Douglas 1952, Public Utilities Commission vs. Pollak

*"The right to be left alone - the most comprehensive of rights, and the right most valued by civilized men."*

-- Supreme Court Justice Louis Brandeis

*"There is no assurance, without scrutiny, that all keying material introduced during the chip programming is not already available to the NSA..... As long as the programming devices are controlled by the NSA, there is no way to prevent the NSA from routinely monitoring all SKIPJACK encrypted traffic. Moreover, compromise of the NSA keys, such as in the Walker case, could compromise the entire EES system."*

-- NASA comments on EES, 1993. ok - branches of the government don't trust the NSA, but we should?

*"Just because you're paranoid doesn't mean some one isn't out to get you..."*

-- Unknown

*"The disk scrambler is of course like any other entity which can be put to good, or bad use (I could perhaps strangle someone with a stethoscope for example....)"*

-- AMAN, 6 July 1998

*"The law does not allow me to testify on any aspect of the National Security Agency, even to the Senate Intelligence Committee."*

-- General Allen, Director of the NSA, 1975

*"You bastards!"*

-- guy@panix.com in response to the above General Allen quote :-)

*"There can be no greater good than the quest for peace, and no finer purpose than the preservation of freedom."*

-- U.S. President Ronald Reagan

*"I know something about trust. I got my trust the old-fashioned way. I earned it."*

-- Bill Clinton, in Federal News Service, 28 October 1992. Hehehehe.

*"The strength of the Constitution lies entirely in the determination of each citizen to defend it. Only if every single citizen feels duty bound to do his share in this defense are the constitutional rights secure."*

-- Albert Einstein

*"It is dangerous to be right when the government is wrong."*

-- Voltaire

*"So far as we are concerned, there is no difference between an encrypted file and a locked suitcase"*

-- UK Customs and Excise official, August 98. Apart from the fact you can force a locked suitcase open :-)

*"If all the personal computers in the world - ~260 million computers - were put to work on a single PGP-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break a single message."*

-- William Crowell, Deputy Director of the National Security Agency, March 1997

*"Without censorship, things can get terribly confused in the public mind."*

-- U.S. General William Westmoreland

*"I would rather be exposed to the inconveniences attending too much liberty than those attending too small a degree of it."*

-- Thomas Jefferson

*"My comment was that the FBI is either incompetent or lying, or both....."*

-- Bruce Schneier on FBI claims that they don't have specialised machines that can break DES

*"But I'd also ask American business not to make a campaign out of just trying to bust through export controls as though somehow there was a God-given, inherent right to send the strongest encryption to anybody in the world, no matter who they are. I don't agree with that. I will never agree with that."*

-- Deputy Secretary of Defense John J. Hamre, 21 July, 1998. *But who said there is a god given right that the DoD can read my messages?*

*"You can torture me all you want, I don't know anything"*

*"torture you... that's a good idea"*

-- Reservoir Dogs (Quentin Tarantino)

*"The NSA response was, 'Well, that was interesting, but there aren't any ciphers like that.'"*

-- Gus Simmons - "The History of Subliminal Channels"

*"A secret between two is a secret of God; a secret among three is everybody's secret."*

-- French proverb (about clipper / key-escrow systems? :-)

*"Can you say 'cryptographic filesystem'? Can you say 'custom filesystem'?"*

-- James MacDonald posting to sci.crypt, August 14, 1998. Sarcastic comment - made unwittingly to the author of ScramDisk :-)

"The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers."

-- Bill Gates from The Road Ahead, p265

"Cryptography is like literacy in the Dark Ages. Infinitely potent, for good and ill... yet basically an intellectual construct, an idea, which by its nature will resist efforts to restrict it to bureaucrats and others who deem only themselves worthy of such Privilege."

-- A Thinking Man's Creed for Crypto

"There is a secret message embedded in the phosphor of this period."

-- David Honig [honig@sprynet.com] .sig

"It's the dungheap of History. If you look really, really closely at the tippy top, you can see Louis Freeh holding a Clipper chip."

-- Xcott Craver posting to sci.crypt 20 August 1998. Describing the 'pyramid thing' on the cover of AC2 :-)

"You shouldn't overestimate the I.Q. of crooks."

-- NYT: Stuart A. Baker, General Counsel for the NSA, explained why crooks and terrorists who are smart enough to use data encryption would be stupid enough to choose the U.S. Government's compromised data encryption standard.

"An essential element of freedom is the right to privacy, a right that cannot be expected to stand against an unremitting technological attack."

-- Whitfield Diffie, Distinguished Engineer at Sun Microsystems

"It must always be remembered that crime statistics are highly inflammatory---an explosive fuel that powers the nation's debate over a large number of important social issues---and that FBI Director Louis Freeh today is the leading official shovelling the fuel into the blazing firebox."

-- David Burnham

"Why should you care if you have nothing to hide?"

-- J. Edgar Hoover

"I love my country but fear my government"

-- Anonymous

"...Finally, face it; PGP, albeit useful for some niche applications, is a little pissant pimple on the body of cryptographic usage."

-- David Sternlight posting to comp.security.pgp.discuss, June 25, 1997. Click [here](#) for more :-)

"Where the hell is your great contribution to the field that I worked in?????"

-- Robert Gifford posting to comp.security.pgp.discuss, Aug 25, 1999 to David Sternlight :-).

"I have not got any father than just a few variables past one round. I tried to search for real info on the 3.5 rounds that some one reverseved engineered but could not find it."

-- The literate David A. Scott posting to sci.crypt , June 26, 1998. RE his analysis of IDEA :-)

"I have developed an encryption software package that I can best describe as a ONE-TIME-PAD GENERATOR."

-- Anthony Stephen Szopa posting to sci.crypt, August 8, 1997

"Is it time for another one of these already? Oh, bother."

-- Bruce Schneier posting to sci.crypt, August 8, 1997 - in response to the Szopa quote :-)

"Quis Custodiet Ipsos Custodes." -> "Who will watch the watchmen."

-- Juvenal, circa 128 AD

*"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."*

-- John Von Neumann, 1951

*"Random numbers should not be generated with a method chosen at random."*

-- Donald Knuth, vol 2.

*"Key escrow to rule them all; key escrow to find them. Key escrow to bring them all and in the darkness bind them. In the land of surveillance where Big Brother lies."*

-- Peter Gutmann

*"When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl."*

-- Kevin McCurleys Thought for the day, June 24, 1997

*"Mary had a little key (It's all she could export),  
and all the email that she sent was opened at the Fort."*

-- Ron Rivest

*"Mary had a crypto key, she kept it in escrow,  
and everything that Mary said, the Feds were sure to know."*

-- Sam Simpson, July 9, 1998

*"There is a group at Fort Meade  
who fear that which they cannot read  
so they fight with their friends  
(God knows to what ends!)  
In attempts to get more than they need."*

-- Jim Bidzos, CEO of RSA Data Security

*"Feistel and Coppersmith rule. Sixteen rounds and one hell of an avalanche."*

-- Stephan Eisvogel in de.comp.security, Jan 1998

*"The NSA regularly lies to people who ask it for advice on export control. They have no reason not to; accomplishing their goal by any legal means is fine by them. Lying by government employees is legal."*

-- John Gilmore (gnu@toad.com)

*"In God we trust. Everybody else we verify using PGP!"*

-- Tim Newsome

*"BTW, I learned a lovely new acronym today: "Law Enforcement Agency Key" - LEAK."*

-- Charles H. Lindsey (chl@clw.cs.man.ac.uk)

*"They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."*

-- Benjamin Franklin

*"Necessity is the plea for every infringement of human freedom. It is the argument of tyrants; it is the creed of slaves."*

-- William Pitt, British Prime Minister, November 18, 1783

*"There's no way to rule innocent men. The only power any government has is the power to crack down on criminals. Well, when there aren't enough criminals, one makes them. One declares so many things to be a crime that it becomes impossible to live without breaking laws."*

-- Ayn Rand, "Atlas Shrugged"

*"This method, seemingly very clever, actually played into our hands! And so it often happens that an apparently ingenious idea is in fact a weakness which the scientific cryptographer seizes on for his solution."*

-- Herbert Yardley, The American Black Chamber, p282, referring to a Japanese method of transposing the sections of a code message to hide the beginning and end.

*"I applied ROT13 to this, but that didn't make it any more intelligible!"*

-- Roger Schlafly posting to sci.crypt, 21st June 98 in response to a message posted in German :-)

*"The Internet treats censorship as a malfunction and routes around it."*

-- John Perry Barlow

*"Liberty means responsibility. That is why most men dread it."*

-- George Bernard Shaw

*"Furem fur cognoscit et lupum lupus. " -> "A thief recognises a thief and a wolf a wolf."*

-- Anon

---

## Contacting the author

The author of the program wishes to remain anonymous for personal reasons. If you wish to get a message to the author, please direct e-mail to the address below, preferably PGP encrypted. Alternatively, send a message to the account [scramdisk@hotmail.com](mailto:scramdisk@hotmail.com), which is read by both AMAN and myself.

Also, the author may be contacted by writing to the sci.crypt or alt.security.pgp newsgroups with the word 'Scramdisk' in the postings Subject heading. The author uses the pseudonym AMAN.

The PGP details for [ssimpson@hertreg.ac.uk](mailto:ssimpson@hertreg.ac.uk) are available from the PGP key server, or from the web page detailed below. Key details are as follow:

Key Type	Size (bits)	Created	Key ID
RSA	2048	22/08/97	0x560D21A9
Diffie-Hellman/DSS	3072/1024	24/07/97	0x433FDB4F

Updates to ScramDisk and details of development efforts can be found at the site: <http://www.hertreg.ac.uk/ss/>

## Acknowledgements

We would like to thank dozens of people for helping the crypto cause, but I haven't got time to type a comprehensive list ☹ Obvious people are Phil Zimmerman, David Kahn, Professor's Bernstein & Junger, James Bamford, Charles (Softwar), Paul Leyland & Ross Anderson for expressing their views on cryptography so well. Then there are the crypto-kings, who develop, cryptoanalyse and intelligently comment on cryptography, the likes of: Matt Blaze, Martin Hellman, Bruce Schneier, John Savard, Don Coppersmith, Ron Rivest, Eli Biham, Ralph Merkle, James Massey and far too many more to mention.

Oh, I should also mention the author of the program, for tirelessly producing and enhancing the program. I am assured that he will deservedly reach the (anonymous) status of net.sainthood, whatever that is!

***Please do not hesitate to contact me with any comments, errors and omissions.***

## Appendix A – Algorithm Test Vectors

Cipher	Source	Reorder <sup>2</sup>	Key	Plaintext	Ciphertext
Blowfish	Counterpane web site	No	00000000	00000000	4EF99745
			00000000	00000000	6198DD78
Blowfish	Counterpane web site	No	FFFFFFFF	FFFFFFFF	51866FD5
			FFFFFFFF	FFFFFFFF	B85ECB8A
Blowfish	Counterpane web site	No	FFFFFFFF	00000000	F21E9A77
			FFFFFFFF	00000000	B71C49BC
DES	<a href="http://www.itl.nist.gov/div897/pubs/fip81.htm">www.itl.nist.gov/div897/pubs/fip81.htm</a>	Yes	01234567	4E6F7720	3FA40E8A
			89ABCDEF	69732074	984D4815
DES	Applied Cryptography 2 <sup>nd</sup> edition, p631	Yes	01234567	01234567	C9574425
			89ABCDEF	89ABCDEF	6A5ED31D
IDEA	Cryptlib Source Code	Yes	00010002	00000001	11FBED2B
			00030004	00020003	01986DE5
			00050006		
			00070008		
MISTY1	MISTY1 RFC	No	00112233	01234567	8B1DA5F5
			44556677	89ABCDEF	6AB3D07C
			8899AABB		
			CCDDEEFF		
Square	<a href="http://www.esat.kuleuven.ac.be/~rijmen/downloadable/square/vdata">www.esat.kuleuven.ac.be/~rijmen/downloadable/square/vdata</a>	Yes	80000000	00000000	05F8AAFD
			00000000	00000000	EFB4F5F9
			00000000	00000000	C751E5B3
			00000000	00000000	6C8A37D8
TEA32	Sci.crypt	No	00000000	00000000	41EA3A0A
			00000000	00000000	94BAA940
			00000000		
			00000000		
TEA32	Sci.crypt	No	4C617073	4561726C	4B20E121
			616E675F	47726579	C32E8546
			536F7563		
			686F6E67		

<sup>2</sup> This column indicates whether you need to tick the "Read byte values from left to right in memory order" check box in order to correctly verify the test vectors.